CLOUDFLARE

RESUMEN DE SOLUCIÓN

¿Cómo ayuda una autenticación sólida a detener los ataques de phishing?

Las claves de seguridad y un enfoque Zero Trust pueden detener a los phishers.

La amenaza que supone el phishing

Pérdida de datos, redes en riesgo, robo de cuentas

Los ataques de phishing selectivo son uno de los vectores de amenaza más peligrosos a los que se enfrentan las organizaciones en la actualidad. El objetivo de los ataques de phishing y de ingeniería social es manipular a los usuarios para que les proporcionen información confidencial o acceso. Las credenciales de inicio de sesión son un objetivo común.

El éxito de ataques de este tipo puede causar:

- Apropiación de cuentas
- Un enlace en un ataque mayor a la cadena de suministro
- La exfiltración de datos como información de identificación personal y direcciones IP
- Ataques de malware como ransomware

Afortunadamente, hay soluciones muy efectivas disponibles para reducir el riesgo de phishing. Una de las más importantes es la autenticación multifactor (MFA).

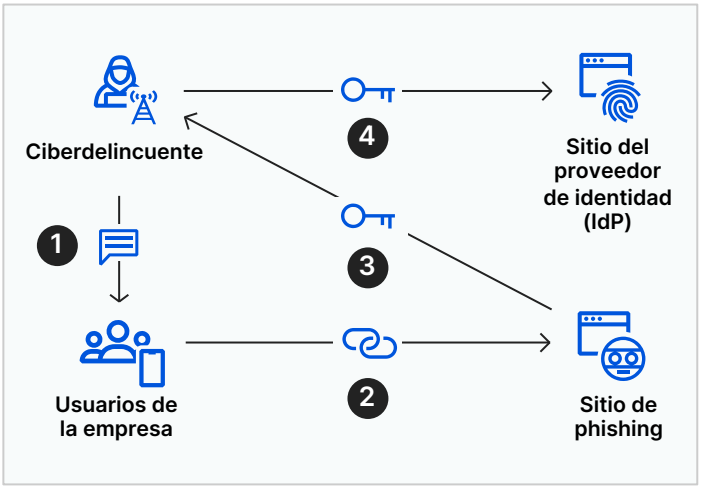


Figura 1: Anatomía de un ataque de phishing mediante SMS. 1. Envío de un mensaje de texto de aspecto legítimo. 2. Enlace a un sitio de aspecto legítimo. 3. En tiempo real, transmisión de la contraseña de un solo uso de duración definida y de las credenciales de la víctima. 4. Inicio de sesión en el sitio real del proveedor de identidad de la empresa.

Cómo ayuda la autenticación multifactor a evitar el phishing

MFA neutraliza el robo de contraseñas

MFA requiere que, para iniciar sesión, los usuarios presenten una clave además del nombre de usuario y
la contraseña. Sin esta clave, ni ellos ni un atacante pueden acceder a las cuentas.

MFA con claves temporales

Una implementación común de MFA es utilizar claves temporales como contraseñas de un solo uso de duración definida (TOTP). Las TOTP a menudo se envían mediante un mensaje SMS, un correo electrónico o aplicaciones. Aunque son más seguras que la autenticación de factor único, los atacantes pueden interceptarlas.

MFA con claves de seguridad

Un atacante no puede interceptar las claves de seguridad compatibles con FIDO2 una vez emitidas. Robarlas es prácticamente imposible sin acceder a ellas físicamente. Investigaciones de Google han concluido que el uso de claves de seguridad compatibles con FIDO2/U2F bloquea el 100 % de los intentos de apropiación de cuenta.

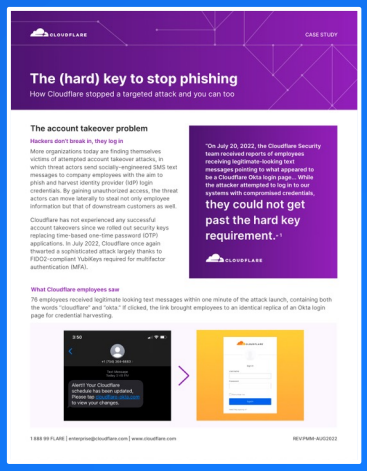
Aplica un sistema de autenticación sólida de manera selectiva

Algunas soluciones de gestión de identidad y acceso (IAM) pueden admitir una autenticación sólida, pero no permiten a los administradores exigir este requisito. Con ZTNA, puedes exigir la autenticación FIDO2, especialmente para aquellas aplicaciones que alojan datos confidenciales. Cloudflare requiere MFA de clave de seguridad para cada autenticación, lo que ha reforzado considerablemente nuestra postura de seguridad.

"El 20 de julio de 2022, empleados de Cloudflare informaron a nuestro equipo de seguridad sobre mensajes de texto de aspecto legítimo que estaban recibiendo y que apuntaban a lo que parecía ser una página de inicio de sesión de Cloudflare-Okta. Si bien el atacante intentó iniciar sesión en nuestros sistemas con credenciales en peligro,

no pudo eludir los requisitos de clave de seguridad". [2]

CLOUDFLARE



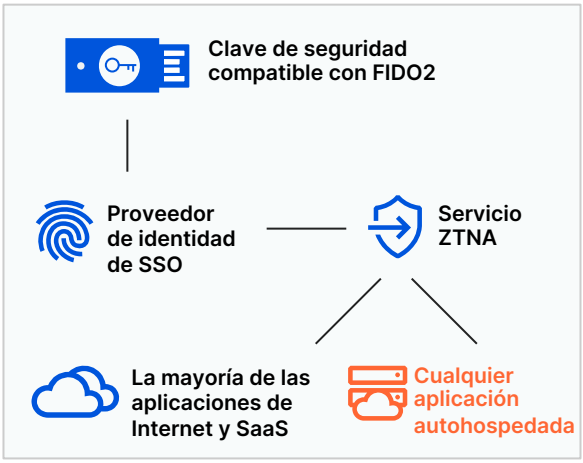
Implementa una autenticación sólida en todas partes

MFA compatible con FIDO2 para todas tus aplicaciones

Es posible aplicar MFA para servicios en la nube de diversas formas tradicionales, especialmente con un servicio de inicio de sesión único (SSO). Pero esto puede resultar difícil con las aplicaciones heredadas o no web, muchas de las cuales no admiten este tipo de autenticación de forma nativa.

Simplifica la implementación con ZTNA

El acceso a la red Zero Trust (ZTNA) funciona como una capa de agregación para todos tus recursos y permite políticas de autenticación estricta para cada uno de ellos. Tanto las aplicaciones SaaS, como las autohospedadas y no web pueden ubicarse detrás de ZTNA, que facilita la implementación de una autenticación sólida en todas las aplicaciones.



Claves para la implementación de un sistema de autenticación sólida

1

Centraliza la IAM

Centraliza la IAM para que la implementación de MFA en todas las aplicaciones sea más sencilla.

2

Aplica MFA de forma selectiva

Establece la aplicación selectiva de opciones de MFA (TOTP y FIDO2 o solo FIDO2) según la identidad y el contexto.

3

Admite dispositivos móviles

Facilita soluciones FIDO2 para portátiles, ordenadores de escritorio y servidores, así como para dispositivos móviles.

1. krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/
2. Publicación del blog de Cloudflare, 9 de agosto de 2022, "Dinámicas de una estafa de phishing sofisticada y cómo la detuvimos", blog.cloudflare.com/2022-07-sms-phishing-attacks/